IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

RMAIL LIMITED, Plaintiff, v. AMAZON.COM, INC. and , PAYPAL, Defendants.	Case No. 2:10-CV-258-JRG (Lead Case) Hon. Rodney Gilstrap
RPOST HOLDINGS, INC., RPOST INTERNATIONAL LIMITED, and RMAIL LIMITED, Plaintiffs, v. READNOTIFY.COM PTY LTD. and CHRIS DRAKE, Defendants.	Case No. 2:11-cv-16-JRG
RPOST HOLDINGS, INC., RPOST INTERNATIONAL LIMITED, and RMAIL LIMITED, Plaintiffs, v. ZIX CORPORATION, Defendants.	Case N0. 2:11-cv-64-JRG

RMAIL LIMITED, RPOST COMMUNICATIONS LIMITED, and RPOST HOLDINGS, INC., Plaintiffs, v. DOCUSIGN, INC., Defendant.	Case No. 2:11-cv-299-JRG
RMAIL LIMITED, RPOST COMMUNICATIONS LIMITED, and RPOST HOLDINGS, INC., Plaintiffs, v. RIGHT SIGNATURE, LLC, FARMERS GROUP, INC., and FARMERS INSURANCE COMPANY, INC., Defendants.	Case No. 2:11-cv-300-JRG
RPOST HOLDINGS, INC., RPOST COMMUNICATIONS LIMITED, and RMAIL LIMITED, Plaintiffs, v. ADOBE SYSTEMS INCORPORATED and ECHOSIGN, INC. Defendants.	Case No. 2:11-cv-325-JRG

PLAINTIFFS' OPENING CLAIM CONSTRUCTION BRIEF

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

TABLE OF ABBREVIATIONS AND LABELS

’219 patent	U.S. Patent No. 6,182,219 B1 and/or C1 (depending on context)
’334 patent	U.S. Patent No. 6,571,334 C1
Feldbau patents	The ’219 and ’334 patents

The Feldbau patents are Exhibits 3 and 4.

’624 patent	U.S. Patent No. 7,707,624 B1
’557 patent	U.S. Patent No. 7,865,557 B1
’372 patent	U.S. Patent No. 7,966,372 B1
Tomkow patents	The ’624, ’557 and ’372 patents

The Tomkow patents are Exhibits 7, 8 and 9

The patents-in-suit	The Feldbau patents and the Tomkow patents

I. INTRODUCTION

Consolidated Plaintiffs submit this Opening Brief in support of their proposed claim constructions, which the Court should adopt over the internally inconsistent and legally flawed claim constructions proposed by the Consolidated Defendants. Plaintiffs' arguments are made with reference to side-by-side comparisons of the disputed constructions, which are in Exhibits 1 and 2. As noted below, for many of the disputed terms, the Defendants themselves cannot agree on the proper construction.

II. FACTUAL BACKGROUND

A. RPost and its Innovations

Plaintiffs are part the RPost Group of Companies, which is referred to commercially as RPost. RPost, which stands for "Registered Post," developed and launched a Registered Email® service in 2000.[1] The company's founders foresaw that electronic mail could replace regular mail for many business practices. RPost's innovative technologies addressed longstanding, but unsolved, problems by verifying what electronic content was sent and received, by whom and to whom, and when, in an innovative and elegant service offering.[2] Over the past thirteen years, RPost has set the global standard for proof records in electronic messages.[3] Ninety of the top 100 U.S. insurance firms use RPost services, as do law firms, telecommunications operators, government agencies, and Fortune 100 companies.

RPost holds 46 patents and has pending applications in 21 different countries.[4] RPost's patents and pending applications broadly cover technologies for providing

[1] http://www.rpost.com/about-rpost/corporate-overview

[2] *Id.*

[3] *Id.*

[4] http://www.rpost.com/about-rpost/intellectual-property/patents

verifiable proof of electronic message transmission and delivery and together apply to virtually all forms of third-party authentication of electronic messaging.[5] RPost asserts five of its patents in the consolidated action. A chart showing the asserted claims against the various Defendants is attached as Exhibit 11.

B. The Feldbau Patents

i. The ’219 patent

The ’219 patent[6] addresses the problem of proving that a sender of a transmission sent it to a particular destination at a particular time and that it had particular content.[7] It solves this problem by, among other things, having the sender transmit the contents to a non-interested third party.[8] The third party associates information such as a time of its successful transmission and its contents to generate evidence capable of proving the dispatch and the contents of the dispatch – “authentication-information.”[9] The later step of testing for a match is called “verification,” at least in the Feldbau patent context.[10]

The ’219 patent further teaches how to render this information indicative of tampering.[11] The third party secures the information against tampering by the sender and the recipient either by storing the information in a secure storage unit, or by using mathematical association methods that would make any tampering easy to detect.[12] Such mathematical association methods may involve digital signatures, encryption or a one-

[5] *Id.*
[6] Ex. 3.
[7] *See, e.g., id.* at 1:30-32.
[8] *See, e.g., id.* at 4:19:29.
[9] *See, e.g., id.* at 2:56-61, 3:22-24, 24:14-21.
[10] *See, e.g., id.* at 13:42-47
[11] *See, e.g., id.* at 10:13-13:7; 14:25-14:57.
[12] *See, e.g., id.* at 7:41-58.

way hash.[13] Repeated uses of the same hash function on the same set of data should result in the same relatively small digital output every time.[14]

Recently, the USPTO issued an Ex Parte Reexamination Certificate for U.S Patent No. 6,182,219 confirming the validity of all of the claims.[15] Although the certificate slightly amends the asserted claims of the ’219 patent, when properly construed, the scope of those claims did not change.[16]

ii. The ’334 patent

The ’334 patent is a continuation of the ’219 patent, meaning its specification is identical to that of the ’219 patent. [17] Many of the claim terms overlap. Like the ’219 patent, the ’334 patent has been unsuccessfully attacked in two reexaminations. In the first, all of its claims were confirmed.[18] In the second, which is still pending, its claims were amended in largely the same way as the ’219 claims were amended during reexamination (*i.e.*, in a way that does not change its actual court-interpreted scope). The USPTO recently issued its “Right of Appeal Notice”—the final step before either appeal by the requester (eBay, Inc.—Paypal’s parent company), or issuance of the ’334 patent’s second reexamination certificate.

C. The Tomkow Patents

i. The ’624 patent

The Tomkow patents all relate to verifying the delivery and content of an electronic message. Although the ’624 patent stems from a different parent application

[13] *See, e.g., id.* at 10:47-11:2.
[14] *See, e.g., id.* at 11:15-27.
[15] *See* Ex. 3, attaching the C1 reexamination certificate.
[16] Dkt. Nos. 217, 225.
[17] Ex. 4.
[18] Ex. 4, attaching the C1 reexamination certificate.

than the ’372 and ’557 patents, 11 of its 13 figures, and hence the majority of its disclosure, come from the parent application that led to the ’372 and ’557 patents.[19] The ’624 patent also discloses an additional embodiment for proving the transmission and content of a reply to an electronic message (Figures 12 and 13) that is not found in the ’372 and ’557 patents. The ’624 patent addresses the problem of verifying the content and delivery of a reply to an electronic message by, among other things, having the recipient register his or her reply to an electronic message with a system that provides the recipient proof of receipt and content of the reply.[20] This proof may take the form of a delivery receipt that indicates that the reply was delivered to the sender, which may be transmitted to the recipient. [21]

ii. The ’372 patent

The ’372 patent also addresses the problem of verifying the content and delivery of an electronic message by, among other things, having the sender transmit the message to a server displaced from a destination server. [22] The server returns an electronic receipt to the sender, which may include the message and its attachments, a digest of the message and its attachments, and a portion of a mail transport protocol dialog exchanged between the server and the destination server.[23] The sender may later submit the receipt to the server in order to verify the content and delivery of the message.[24]

[19] Ex. 7 at 7:41-8-16.
[20] *Id.* at 30:44-51.
[21] *Id.*
[22] Ex. 8 at 1:16-21.
[23] *See, e.g., id.* at 3:25-35.
[24] *Id.*

iii. The ’557 patent

The ’557 patent is a divisional application of the same parent application that led to the ’372 patent. The ’557 patent also relates to verifying the delivery and content of electronic messages transmitted from a sender through a server to a recipient.[25] The server generates verifiers for the message and any attachments and provides them to the sender.[26] If the sender later wishes to obtain authentication of the message, for example if there is a dispute that the recipient received the message, the sender transmits the message, the attachments, and the verifiers to the server.[27] The server operates on the message and the message verifier to verify the message and operates on the attachment and the attachment verifier to verify the attachments.[28]

III. LEGAL STANDARDS

Claim construction is “a question of law, to be determined by the court.”[29] A court’s claim construction analysis must begin with the words of the claims themselves, both asserted and unasserted.[30] The Court need not provide a new definition or rewrite a term when the Court finds the term’s plain and ordinary meaning is sufficient.[31] “Plain meaning” claim terms may often go into the jury instructions without explanation.[32]

“It is always necessary to review the specification to determine whether the inventor has used any terms in a manner inconsistent with their ordinary meaning.”[33] However, there is a distinction between proper use of the specification to analyze the

[25] Ex. 9 at 1:16-19.
[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] *Markman v. Westview Instruments, Inc.*, 517 U.S. 370, 384 (1996).
[30] *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582-83 (Fed. Cir. 1996).
[31] *Network-1 Sec. Solutions, Inc. v. Cisco Sys., Inc.*, 692 F. Supp. 2d 632, 648 (E.D. Tex. 2010).
[32] *Sulzer Textil A.G. v. Picanol N.V.*, 358 F.3d 1356, 1367 (Fed. Cir. 2004).
[33] *Vitronics*, 90 F.3d at 1582.

claim, versus improper incorporation of limitations from the specification into the claim language.[34] The prosecution history "represents an ongoing negotiation between the PTO and the applicant, rather than the final product of that negotiation, [such that] it often lacks the clarity of the specification and thus is less useful for claim construction purposes."[35] For reexaminations in particular, the prosecution history might reveal a "negotiation" between a patentee and an examiner which, in effect, simply aligns the USPTO's "broadest reasonable construction" of claim terms with the narrow scope a court would have already given their pre-amendment form.[36]

A court may also consider extrinsic evidence, "which consists of all evidence external to the patent and prosecution history, including expert and inventor testimony, dictionaries, and learned treatises."[37] However, extrinsic evidence should not be used "to contradict claim meaning that is unambiguous in the light of intrinsic evidence."[38] Even inventor testimony cannot be used to contradict the rest of the intrinsic record.[39]

IV. FELDBAU PATENTS ARGUMENT

A. Central Terms of the Feldbau Patents

i. "Authenticate the dispatch . . ."/"authentication-information"[40]

The action verb "authenticate," and the result of the action labeled "authentication-information," must be understood together. One of the central tasks of the '219 patent is to create "authentication-information." Authentication-information is a combination of certain data that "may serve as evidence of both the dispatch and its

[34] *Phillips v. AWH Corp et al.*, 415 F.3d 1303, 1323 (Fed. Cir. 2005).
[35] *Id.*
[36] *See generally*, Manual of Patent Examining Procedure § 2111.
[37] *Phillips*, 415 F.3d at 1317-19.
[38] *Id.* at 1324.
[39] *Vitronics*, 90 F.3d at 1584.
[40] Ex. 2, numbers 18 and 24.

contents."[41] Such information provides a party to the transmission with "evidence" that has the "capability" of proving both the dispatch and its contents.[42] Generating the information "authenticates" a message.[43] In the lexicon of the '219 patent, merely having that evidence available supplies such "authentication."[44] The later step of actually using and testing that information against another set of data is called "verification."[45]

For its contentions, RPost chose wording for the "authenticate/authenticating" phrases that reflects the exact sense of how "authentication" is understood in the '219 patent specification. Likewise, RPost chose wording for the proper construction of "authentication-information" by adopting the Central District of California's exact wording from a 2005 litigated claim construction.[46] Indeed Zix actually agrees with RPost on "authentication-information." The other Defendants' competing and mutually contradictory constructions lack merit for several reasons.

First, the act of "authentication" in the '219 patent's usage is never to "reliably determine the content" of information, as certain Defendants mistakenly state. It is instead to generate evidence capable of proving the content, and whose mere existence instills confidence in the transmission. Even the later, optional, "verification" mechanism cannot of itself determine the content of a dispatch. It can only test whether there is a match between purported content and dispatch information, and actual content and dispatch information. Verification as a process might use authentication-information to

[41] Ex. 3, at 3:29-36.

[42] *Id.* at 2:56-61, 3:22-24.

[43] *Id.* at 5:63-6:6 (envelope 32 comprises "authentication-information" by its mere existence); 9:56-66 (transmitted information "can be authenticated" by having a file server or mail manager with a secure time generator store message content with dispatch information in a secure manner).

[44] *Id.* at 15:8-19, "data authentication" described as being performed by a computation using a private key to encrypt specific kinds of data.

[45] *Id.* at 13:42-47, discussing verification mechanism; *see also* claim 53, a dependent claim with a follow-on verifying step; *see also* Figs. 5-6 and accompanying text, describing a verification mechanism.

[46] Ex. 5.

prove the content, but neither the "authentication" act nor the authentication-information output can do so by itself. They certainly cannot "indisputably prove" the content as RightSignature argues. In the '219 patent, "verification" is not the same thing as "authentication;" it is optional (*e.g.,* in dependant claim 53), and occurs later in time as a completely separate process.

Second, Defendants incorrectly construe the '219 patent reexamination as having altered the proper interpretation. Defendants argue that the time of a *recipient's receipt* of a dispatch must somehow be incorporated into the "authentication" process and the resulting "authentication-information." Defendants are wrong. They overlook the language from elsewhere in the claims indicating that the "time" indicia that becomes associated into the authentication-information is the time of the "successful transmission" of the dispatch by the dispatcher. A time of "successful transmission" is not the same thing as a time of receipt (or delivery). The '219 patent specification confirms this point.

Defendants have relied upon a portion of the '219 patent concerning an optional and distinct aspect of the disclosed embodiments that provides "information 708 indicating the success (or failure) of the message *delivery*."[47] But this optional delivery-information feature—requiring active feedback from a recipient or a recipient system—has nothing to do with the pertinent claim scope either before or after the reexamination amendments. It relates to the success or failure of the message delivery, not the success or failure of the message transmission. While the concepts are loosely related, a "successful transmission" and a "successful delivery" are not one and the same, and indeed the '219 patent describes them each in different ways.

[47] Ex. 3 at 16:3-8, emphasis added by RPost.

The ’219 patent describes how an authenticator of the preferred embodiment determines whether a transmission was successful or not (and therefore, whether to generate authentication-information). This determination considers things happening solely within the authenticator itself and is not dependent on feedback from the recipient:

> The transmission completion indication 64 provides information regarding the success of the transmission. *It is typically obtained from the communication protocol used by the transceiver 76*. It may be for example in the form of an electronic signal *provided by the transceiver 76* which is used to determine the validity of the rest of authentication-information, or in a form similar to that provided in transmission reports such as “TRANSMISSION OK” or “ERROR”.[48]

This excerpt shows that an indicia of a successful transmission relates to activities at the authenticator without regard to delivery success or failure. The transceiver 76 is something wholly within authenticator 70 (*see* Figure 2). Thus, in sending the message, the authenticator of this embodiment notifies itself of affirmative completion. Conversely, the reexamination file history confirms that the claims do not cover systems that require the recipient’s cooperation to construct evidence of the *transmission*.[49] Even if there were any doubt, dependent claims 69, 79 and 88 permit a “delivery indicia” to become part of the “authentication-information.” Thus, the independent claims do not incorporate the limitation of delivery indicia, or any notion of a successful delivery.[50]

For all these reasons, neither the “authenticate” phrase nor “authentication-information” in the independent claims properly incorporates any connotation of actual receipt or delivery of a dispatch at a destination.

[48] Ex. 3 at 7:29-40, emphasis added.

[49] Exhibit 6, March 29, 2012 Response at 31.

[50] *See Charles E. Hill & Assocs. v. Abt Elecs., Inc.*, 2012 U.S. Dist. LEXIS 3026, at *21-22 (E.D. Tex. Jan. 10, 2012).

ii. "Dispatch"[51]

RPost contends that a "dispatch" does not need construction because it's a plain English word that is easily understood from its context within the patent claims, namely "the transmission sent from a sender to a recipient via a dispatcher." Defendants' six competing and mutually inconsistent constructions should be rejected.

First, Amazon and Paypal are wrong that a "dispatch" must contain "the sender's message and the destination information." For one thing, no independent claim contains the term "message" anywhere within it. The independent claims are deliberately broader than this, using the label "content" for the information originated by the sender. Nor should "the destination information" be improperly imported into the term "dispatch," since the concept of destination information already appears elsewhere in each independent claim. Notably, defendant Zix agrees with RPost on this point, and disagrees with its co-defendants, since Zix's construction is the same as Amazon's and Paypal's except for omitting the unneeded limitation of "the destination information."

Second, ReadNotify asserts the same unnecessary limitations as Amazon and Paypal ("message" and "destination information"). ReadNotify also incorrectly omits the connotation that "the dispatcher" sends along the transmission as an intermediary (a mistake that Amazon and Paypal do not make). This connotation is explicit in independent claims 1 and 30, whose preamble denotes that the dispatch is sent "via a dispatcher." That connotation arises because a "dispatch" in its plain meaning is already known to be something relayed from a sender to a recipient through an intermediary.

Adobe (like Zix) does not import "destination information" into "dispatch". However, Adobe makes the two other errors discussed above, namely (a) using the notion

[51] Ex. 2, number 12.

of a "message" instead of the deliberately broader term "content," and (b) omitting the connotation that the dispatch is sent "via a dispatcher."

Docusign and RightSignature improperly import a "store and forward" limitation into "diaptach." But the drafters deliberately omitted this terminology from the claims. And strangely, despite their correct understanding that a "dispatch" is something that is "forwarded," Docusign and RightSignature incorrectly omit the entity doing the forwarding (a dispatcher) even though it is both implicit in the term "dispatch," and written explicitly into several independent claims. Docusign and RightSignature also seek a limitation requiring identity between the sent data and the received data, a notion foreign to the simple term "dispatch."

Finally, Chris Drake improperly loads "dispatch" with connotations already existing elsewhere in the independent claims ("successful transmission" and "non-interested third party"). He also mistakenly contends that "dispatch" is "an act" (a verb). In the claims, a "dispatch" is a transmission (a noun), not an act: *e.g.*, claim 30, "a3 – information describing the destination of said dispatch."

iii. "An indicia of a time of successful transmission . . ."[52]

As with "dispatch," Defendants are in sixfold disagreement over the proper construction of the "time indicia" terms. RPost has pinpointed the exact "time" indication that the claims address—an indicia of the time of the dispatcher's successful transmission of the dispatch to the recipient.

The common mistake among all Defendants is misreading "transmission" by the intermediary as "receipt" or "delivery" at the destination. As discussed above, a "successful transmission" is one that actually gets sent out from the

[52] Ex. 2, number 13.

dispatcher/authenticator toward the recipient, regardless of whether delivery ever occurs. Delivery is a separate concept from transmission. The patent specifications treat them differently. Dependent claims 69, 79 and 88 of the '219 patent separately claim the distinct (and optional) notion of delivery indicia. While the Feldbau patents do treat a successful transmission as a proxy for a successful delivery,[53] that does not justify importing delivery-based limitations into a claim that explicitly uses the phrase "successful transmission," not "successful delivery" or "successful receipt."

iv. "Resistant to or indicative of tampering . . ."[54]

RPost relies on plain and ordinary meaning for its construction of "resistant to or indicative of tampering by either of the sender and the recipient." "Resistant to . . . tampering" means it is "difficult" to tamper. "Indicative of tampering" means that tampering is detectable. The '219 patent (Ex. 3) provides the two nonlimiting examples of how this is done at col. 7, ll. 41-58: secure storage and mathematical association.

It is not clear whether Defendants dispute RPost's construction. The construction offered by Amazon and Paypal simply refers back to a prior disputed term, where they offer no explicit interpretation. The Adobe/DocuSign/RightSignature/ReadNotify/Zix construction correctly summarizes the objects or goals of this limitation, but omits any expression of what the term itself might mean (much less any mechanism for achieving the goal). As an explanation for the jury, this construction is confusing and inadequate. Thus, the Court should adopt RPost's construction.

[53] Ex. 3 at 17:55-57.
[54] Ex. 2, number 30.

v. "Authenticator"[55]

The CDCAL has already held that an "authenticator" is "[a] subsystem that operates to authenticate a dispatch and functions as a noninterested third party with respect to the sender and the recipient."[56] RPost added the sense that it must be a "digital electronic" subsystem to match how the term is used in the '219 patent. In Rmail's response to Paypal's motion for summary judgment under 35 U.S.C. § 101, Rmail pointed out why it was appropriate to add the "digital electronic" sense of the term to the construction: that (1) the human-only embodiment of the ideas of the '219 patent did not use the term "authenticator," and was not claimed; (2) the electronic-only embodiments do use the term "authenticator;" (3) the broadest usage of the term "authenticator" denotes an "apparatus" that is "constructed" and is "electronic;" (4) the originally-filed claims did not have "authenticator" language because that was added later by amendment; and (5) other amendments confirmed that the electronic information that the authenticator operated upon was "data," connoting something "digital." Therefore, it is appropriate to modify the CDCAL's construction of "authenticator" as a "digital electronic" subsystem. [57]

Defendants omit the "digital electronic" sense of the "subsystem," but that is clearly wrong, as noted above.[58] Defendants in some cases note that the "authenticator" is the subsystem that "generates" the authentication-information, and does so without sender/recipient cooperation, but this is already implicit in RPost's construction that the

[55] Ex. 2, number 22.
[56] Ex. 5, at 4-7, 14.
[57] Dkt. No. 98, at 6-11.
[58] Dkt. No. 98.

authenticator performs the authentication function, and does so as a non-interested third party (separately construed in the next section).

vi. "Non-interested third party"[59]

RPost contends that a "non-interested third party" in the Feldbau patents does not need construction because it is a plain phrase that is easily understood by a lay person. Its meaning is clear from its context within the patent claims, namely a party without an interest in the outcome of the function it is performing. The CDCAL held that "[the authenticator] functioning as a non-interested third party with respect to the sender and recipient" connotes "[t]he authenticator functions like an unbiased party would function with respect to the sender and the receiver, in carrying out the operations of the authenticator, and carries out its authentication function without the participation of the sender or the recipient."[60] With slight reordering of the terms to enhance clarity, RPost's construction is the same.

Defendants try to urge two changes to this earlier court outcome. First, rather than connoting the performance of the authentication function "without the participation" of the sender and receiver, they impose a limitation that it is "without the cooperation" of the sender and receiver. This detracts unnecessarily from the clarity of the earlier construction. Defendants do not explain why the CDCAL's decision explaining that the task occurs "without the participation" of these parties is inadequate in any way, or requires such drastic changes.

Second, where the CDCAL was careful to note that the authenticator is "unbiased . . . in carrying out the operations of the authenticator," Defendants convert this into the

[59] Ex. 2, numbers 4 and 23.
[60] Ex. 5, at 14.

authenticator having “no interest in the dispatch.” It is not clear what Defendants hope to achieve with this second linguistic shift. But RPost is concerned that any entity that has a profit motive will, in some fashion, have an “interest” in the transactions it processes. That is not the sense of the Feldbau patents. For the Feldbaus, what was important is that the generation of authentication-information itself was not biased in favor of a sender or a recipient. RPost’s and the CDCAL’s constructions captures this sense, while Defendants’ construction distorts it to achieve undisclosed ends. Accordingly, RPost requests that the Court adopt its construction.

B. Means Plus Function Corresponding Structures

The parties identified two limitation subject to 35 U.S.C. §112(6), located in claims 71 and 82 of the ’219 patent. The first has two forms, since its language was amended during reexamination:

Means for providing an indicia relating to a time of transmission of the dispatch, said time related indicia being provided in a manner resistant to or indicative of tampering by either of the sender and the recipient. ’219 patent, claims 71, 82	Means for providing an indicia of a time of successful transmission of the dispatch to the [destination] receiving system, said time related indicia being recorded by the authenticator and provided in a manner resistant to or indicative of tampering by either of the sender and the recipient. ’219 patent reexamination certificate, claims 71, 82.

The second has only one form in each of claims 71 and 82, since it is identical both before and after reexamination:

Means for securing at least part of the authentication data against tampering of the sender and the recipient[, the authenticator functioning as a non-interested third party with respect to the sender and the recipient] / [wherein the processor is combined with the means for securing]. ’219 patent, original and reexamination certificate, claims 71, 82.

Here, for the first means limitation above (“means for providing,” in both its forms), RPost identified “an internal clock 50 located within the authenticator or an externally obtained time source that is secured from being set by an interested party such as the sender." For the second ("means for securing"), RPost identified "a storage unit 54 or storage device 106 that may be a write-once read-many (WORM) device such as an optical disk or a Programmable Read-Only Memory device, it may be enclosed within a securable device, or it may be provided with read-only access privilege. Alternatively, the storage unit or storage device may store authentication-information using a compression, private or public key encryption or scrambling technique, a password, or a combination thereof."

There can be no question that RPost is correct, that "internal clock 50" is the structure in the specification that provides the noted time indicia. That is clear at least from col. 7, ll. 12-28. For example, this passage begins, "The internal clock 50 provides an indication 66 of the current time, and is utilized to provide a time indication for the transmission." This sentence uses some of the exact words of the function part of the limitation. Likewise, the disclosure from col. 7 lays out the "alternative" structure of an externally obtained time indication 66.

There can also be no question that RPost is correct about the means for securing. That is clear at least from col.7, ll. 41-58. This passage includes the following text: "Typically the storage unit 54 is relatively secure, such that the authentication-information contained therein is assumed unchangeable. For example it may be a Write-Once-Read-Many (WORM) device such as an optical disk or a Programmable Read-Only Memory (PROM) device, it may be enclosed within a securable device, or it may be provided with read-only access privilege." Likewise, this excerpt lays out the "alternative" structure that "the authentication-information is stored in a secure manner, for example using a compression, private or public key encryption or scrambling technique, a password, or a combination thereof, such as those . . . where the 'securing' procedure, key or password are unknown to any interested party."

Defendants wrongly assert that no corresponding structure is disclosed for the post-reexamination form of "means for providing." Defendants have never explained their contention. They have overlooked the specification, as considered above.

C. Other Terms of the Feldbau Patents

RPost believes that the vast majority of the remaining disputes will be predetermined upon the Court's resolution of the six central disputes that RPost has identified above. RPost therefore suggests three possible approaches for handling the remainder of the disputed terms. One, the Court may resolve the central disputes noted here and direct the parties to prepare an agreed order expressing how those resolutions have determined the remainder. Two, after considering the central disputes noted here, Defendants' response, RPost's reply, and arguments at the *Markman* Hearing, the Court may proceed workmanlike through the Local Rule 4-5(d) Claim Construction Chart and issue a comprehensive decision announcing the respective rulings of the Court. Or three, if Defendants agree and if the Court permits, the remainder of the disputes may be postponed until the jury instruction conference.

V. TOMKOW PATENTS ARGUMENT[61]

A. Terms of the '624 Patent

i. "a message"[62]

The Court should properly construe "a message" to mean "an electronic message" rather than limit it to "an email"—a type of electronic message—as Defendants contend.

[61] Ex. 1 is a side-by-side comparison of the disputed Tomkow patent terms grouped by issue.

[62] Ex. 1 at p. 1.

Claim 1 distinguishes between "an email," which is recited in the preamble, and "a message," which is recited in the claim body.[63] Thus, the plain language of the claim treats a message and an email differently. Although Defendants note that the invention is described with respect to email embodiments,[64] the specification explicitly states that the invention is not limited to a particular message type: "[i]t is to be understood that the particular message type . . . is for illustration only; the invention also applies to other electronic message protocols and message types."[65] Indeed, the title of the '624 patent recites "an electronic message" and 11 out of its 13 figures come from the '372 patent, which, as discussed below, relates to verifying an electronic message, such as an email. Because Defendants improperly limit the term "message" to illustrative embodiments in the specification, their construction must be rejected.[66]

Defendants' construction is also flawed because it adds the limitation "from the sender to the recipient." The plain language of the claims, however, recites that the message passes from the sender to a server or from the server to a recipient.[67] Thus, the term "message" cannot be defined as something that only goes "from the sender to the recipient." For this additional reason, Defendants' construction must be rejected.

ii. "a 'mailto' link"[68]

The Court should adopt RPost's construction of "a 'mailto' link" because it is consistent with the intrinsic record. In describing "a 'mailto' link," the specification

[63] Ex. 7 at 31:65-32:2.
[64] *See, e.g.*, Dkt. Nos. 211-12 and 211-13.
[65] Ex. 7 at 8:40-44.
[66] *Phillips*, 415 F.3d at 1323.
[67] Ex. 7 at 32:1-2, 10.
[68] Ex. 1 at p. 1

states "[w]hen a recipient . . . clicks on the link, the browser will open the recipient's default mail client with a message already addressed to the embedded address."[69]

Defendants' construction, however, improperly limits this term to "an HTML link . . . that specifies the mailto protocol." It is evident from the plain language that claim 1 is not intended to be limited to any particular language or protocol. Indeed, claim 4, which depends from claim 1 states "the message from the sender to the recipient is provided in a particular format at the server."[70] Similarly, unlike claim 1, claim 7 specifically recites "adding an HTML link in the message."[71] Further, the specification specifically states that the invention applies to multiple message types and protocols.[72] Indeed, Figure 12 shows that a link may be added to a message that is MIME or HMTL format.[73] Because there is ample intrinsic evidence that claim 1 is not limited to any particular format or protocol, Defendants' construction must be rejected.

iii. "an invitation to click on the link . . ."[74]

The dispute between the parties concerns however what form "an invitation" must take. Neither the claim language nor the specification place any limits on the type of invitation. Indeed, the specification states that multiple items can perform the act of iniviting: "[a]dditionally, the tag may contain instructions, World Wide web addresses, or links that invite and allow the recipient to send a reply made of record to the message."[75] Defendants' construction, however, improperly limits "an invitation" to text embedded in an email message. Not only is there no such language in the claims, the specification

[69] Ex. 7 at 31:15-18.
[70] *Id.* at 31:38-40.
[71] *Id.* at 33:19.
[72] *Id.* at 8:39-44.
[73] *Id.* at Fig. 12.
[74] Ex. 1 at p.1.
[75] Ex. 7 at 10:44-46.

shows that the invention is not so limited. As such, RPost's plain meaning construction should be adopted Defendants' unduly narrow construction rejected.

iv. "a manually initiated reply"[76]

Defendants' litigation-induced construction of "a manually initiated reply" improperly limits the invention to actions performed by hand, specifically using the hands to click on the "mailto" link. Neither the plain language of the claims nor the specification requires that a user use his hands to click on the "mailto" link. A person of ordinary skill in the art would know that such a link may be selected by other user actions, such as by voice command. Rather, the inventor used the term "manually" to distinguish systems that automatically generate delivery status notifications, not systems that are operated by hand: "[a]pplicant claims a reply that is manually initiated by the recipient of the email, which is completely different from an automatic DSN generated by a recipients email system."[77] RPost's construction is consistent with this intrinsic evidence and should be adopted over Defendants'.

v. "generating a manually initiated reply . . ."[78]

RPost contends that this phrase should be construed according to the plain claim language. Defendants' construction is flawed because it improperly imposes two limitations (1) "clicking the "mailto" link," which as discussed above is unduly limiting and is already recited in the claim, and (2) "manually entering a message into a mail client," which contradicts the plain language of the claims. Claim 11 specifically claims an embodiment of the invention where the recipient composes a reply to the message in a

[76] Ex. 1 at p. 1.

[77] Ex. 10 at p.8.

[78] Ex. 1 at p. 1.

mail client.[79] The absence of this express limitation in claim 1 indicates that claim 1 is not so limited.[80] Because both additional limitations proposed by Defendants contradict the intrinsic record, the Court should reject Defendants' construction and adopt RPost's.

vi. "transmitting the manually initiated reply"[81]

RPost contends that the phrase "transmitting the manually initiated reply to the sender through the server" should be construed according to its plain and ordinary meaning. Defendants' construction, however, reads the "through the server" language right out of the claims. For this reason alone, Defendants' construction is flawed.[82] Not only does the language "through the server" appear in claim 1, it also appears in claim 2, 3, and 6—all of which depend from claim 1.[83] Defendants' construction contradicts this plain claim language and the specification, which indicates that the server sends the manually initiated reply to the sender.[84] Thus, RPost's construction should be adopted.

vii. "an indication that the reply is transmitted or delivered . . ."[85]

RPost contends that the phrase "an indication that the reply is transmitted or delivered to the sender" should be given its plain and ordinary meaning. Because Defendants also agree that the plain and ordinary meaning should control, RPost's construction should be adopted.

viii. "a unique identification . . .," "provided on the basis . . ."

RPost contends that the "unique identification" phrases of the message" should be given their plain and ordinary meaning. Defendants' constructions, on the other hand,

[79] Ex. 7 at 34:27-30.
[80] *See Charles E. Hill & Assocs.*, 2012 U.S. Dist. LEXIS 3026, at *21-22.
[81] Ex. 1 at p. 1.
[82] *Phillips*, 415 F.3d at 1314.
[83] Ex. 7 at 32:30, 34, and 54.
[84] *Id.* at 31:20-28; Fig. 13 1507-1510.
[85] Ex. 1 at p. 2.

rewrite the claim language unnecessarily because they do not appear to change the claim's plain meaning.[86] As such, the Court should adopt RPost's constructions.

ix. "initiating manually a reply to the message by the recipient"[87]

Subject to its co-pending Motion for Leave to Amend Disclosures,[88] RPost requests that the Court construe the "initiating manually" from claim 7 to mean "initiating in response to an action of the recipient a reply to the electronic message." For example, in step 1506, the system initiates a reply to the electronic message in response to an action of the recipient, such as clicking on the HTML link.[89]

B. Terms of the '372 Patent and Common Terms to the '557 Patent

i. "a message" and "an electronic attachment"[90]

The Court should properly construe "a message" to mean "an electronic message" rather than limit it to "an email"—merely one type of electronic message—as Defendants contend. The asserted claims recite "a message" and do not specifically recite an email.[91] Although the specification describes several email embodiments,[92] the invention is not limited to a particular message type, and applies to several other message types:

> the present invention may apply to any electronic message that can be transmitted through a electronic message network or through any electronic gate. Electronic messages may include text, audio, video, graphics, data, and attachments of various file types.[93]

[86] *02 Micro Int'l Ltd. v. Beyond Innovation Tech. Co.*, 521 F.3d 1351,1362 (Fed. Cir. 2008).
[87] Ex. 1 at p. 2.
[88] Dkt. No. 245.
[89] Ex. 7 at 31:15-19; Figure 13.
[90] Ex. 1 at p. 3.
[91] *See, e.g.,* Ex. 8 at 27:63-28:15.
[92] *See, e.g.,* Dkt. No. 211-12, 211-14.
[93] Ex. 8 at 27:63-67.

Indeed, the title of the '372 patent recites "an electronic message" and relates to verifying an electronic message, such as an email.[94] Because Defendants' construction improperly limits the term message to illustrative embodiments, it must be rejected.

Defendants' construction is also flawed because it unaccountably adds the limitation "from the sender to the recipient." The plain language of the claims, however, recites that the message passes from the sender to a server or from the server to a recipient.[95] Thus, the term "message" cannot be defined as something that only goes "from the sender to the recipient."

Finally, the parties only dispute regarding the "attachment" terms is whether it is an attachment to an electronic message (RPost) or an attachment to an email (Defendants). Because a message should be construed to be an electronic message, RPost's construction of "an electronic attachment" should be adopted.

ii. "mail transport protocol dialog" and related terms[96]

RPost contends that the phrase "mail transport protocol" should not be construed because it does not appear in the claims. Instead, the claims recite "mail transport protocol dialog."[97] The claims also state the "mail transport protocol dialog" is a SMTP or ESMTP dialog, not that the "mail transport protocol" is SMTP or ESMTP as Defendants propose.[98] Accordingly, Defendants' proposal improperly construes "mail transport protocol" out of context and conflicts with the plain language of the claims.

Instead, the Court should construe and adopt RPost's construction of "mail transport protocol dialog." RPost's construction is consistent with the plain language of

[94] *Id.* at Title and Abstract.
[95] *Id.* at 27:63-65.
[96] Ex. 1 at p. 3.
[97] *See, e.g.,* Ex. 8 at 28:1-2.
[98] *Id.* at 29:17-20; 30:40-41.

the claims, which state that the mail transport protocol dialog includes "data exchanged between the server and the recipient relating to the message."[99] RPost agrees that the mail transport protocol dialog encompasses commands and responses, as Defendants' propose, but it should not be limited to commands and responses. Rather, as the claim language and the specification makes clear, the mail transport protocol dialog also encompasses other data, such as timestamps: "[s]ince the receipt itself and SMTP dialogs and DSN reports within the receipt contain timestamps, the receipt includes a non-forgeable record of the message recipient(s), the message content, and the time(s) and route(s) of delivery."[100] Because Defendants' construction is unduly narrow, the Court should adopt RPost's construction.

iii. "a digital signature"/"a digital signature of the message"[101]

RPost's construction of "digital signature" is consistent with the intrinsic record, which broadly describes a digital signature as an unique code that may be used to authenticate information contained in an electronic message:

> Additionally, the receipt may include a single overall encrypted message digest or digital signature computed and appended as part of the receipt thus providing a single message authentication code which could be used to authenticate all of the information contained within the receipt.[102]

Defendants' construction, on the other hand, improperly limits the claimed digital signature to an encrypted hash. Although the specification refers to the digital signature as an encrypted hash in a preferred embodiment, the specification provides expressly that an encrypted hash is not the only way to create a digital signature:

[99] *Id.* at 29:17-25; *see also* Ex. 9 at 28:24-28; 28:34-35.

[100] Ex. 8 at 15:45-49; *see also Id.* at 13:1-10.

[101] Ex. 1 at p. 3.

[102] *Id.* at 15:41-45.

> [t]he digital signature can be created using known digital signatures techniques, such as by performing a hash function on the message to produce a message digest and then encrypting the message digest. . . . The encrypted message digest provides one type of message authentication or validation code . . . . Other message authentication and/or validation codes may also be generated and used.[103]

Moreover, and importantly, the claims never refer to the digital signature as an encrypted hash. Thus, Defendants' construction improperly excludes other forms of digital signatures from the scope of the invention.[104] Some of the Defendants also inexplicably attempt to import the limitation "with a private key know only to the party that creates the digital signature," which is only described in the embodiments shown in Figures 2E, 6, and 9. Because the intrinsic record makes clear that the claims are not limited to a particular embodiment, Defendants' construction must be rejected in favor of RPost's.

iv. "authentication/authentication of the message"[105]

RPost's construction of "authentication" and "authentication of the message" are consistent with the intrinsic record, which repeatedly refers to authentication in the context of verifying the content and delivery of an electronic message.[106] In a preferred embodiment, authentication is accomplished through a receipt, which is provided to the originator of the electronic message.

> To later verify and authenticate information contained in the receipt, the originator or user sends a copy of the receipt to the system. The system then verifies that the digital signature matched the original message and the rest of the receipt. If the two match, then the system sends a letter or provides other conformation of authenticity verifying that the electronic message has not been altered.[107]

[103] *Id.* at 3:53-62.
[104] *Phillips*, 415 F.3d at 1323.
[105] Ex. 1 at p. 4.
[106] Ex. 8 at 3:6-9.
[107] *Id.* at 3:28-35.

Conversely, Defendants' construction contains multiple flaws. First, authentication by comparing digital fingerprints is claimed in dependent claims 12 and 22.[108] Thus, independent claims 1 and 16, respectively, cannot be so limited.[109] Second, Defendants' construction requires comparing two digital fingerprints. But the embodiments disclosed in the specification, as claimed in claims 12 and 22, require comparing a digital fingerprint and a digital signature.[110] Because Defendants' construction violates basic claim differentiation principles and conflicts with the intrinsic record, it must be rejected.

v. "before any authentication of the message . . ."[111]

The "before any authentication" clauses of independent claims 1 and 16 simply require that the transmitting step occur before any authentication of the message. They do not require the additional step of authenticating the message. This plain reading of claims 1 and 16 is confirmed by dependent claims 3 and 20, both of which specifically recite an authenticating step. [112] The specification also supports this understanding because any authentication (verification) only occurs if a dispute arises, which could be never.[113] Defendants', however, improperly seek to read an unrecited authentication step into independent claims 1 and 16. Not only does Defendants' construction conflict with the plain language of the claims, it also conflicts with one of the objectives of the invention. As such, RPost's construction should be adopted.

[108] *Id.* at 29:26-31; 30:48-55.
[109] *See Charles E. Hill & Assocs.*, 2012 U.S. Dist. LEXIS 3026, at *21-22.
[110] Ex. 8 at 29:26-31; 30:48-55.
[111] Ex. 1 at p. 4.
[112] Ex. 8 at 28:33-34; 30:29-32.
[113] *Id.* at 24:17-21.

vi. "server"[114]

In the claims, a "server" performs numerous operations, including creating an attachment, transmitting the attachment, and storing a portion of the mail transport dialog.[115] RPost's construction encompasses these various tasks. Defendants' construction improperly limits a "server" to providing data to other computers across network and must be rejected.

vii. "transmitting the message"[116]

RPost contends that the phrase "transmitting the message" should be construed according to its plain and ordinary meaning. Defendants' construction, on the other hand, adds the limitations (1) directly and (2) to a mail server responsible for receiving the recipient's email. Defendants provide no support for either of these limitations.[117] Neither independent claim 1 nor claim 16, both of which recite steps at a server, require that a message be directly sent from the server to a recipient's mail server. In addition, claim 1 does not recite a recipient's mail server at all. Because Defendants provide no basis for deviating from the plain meaning, RPost's construction should be adopted.

viii. "storage means"[118]

Although the parties agree that the term "storage means" should be governed by 35 U.S.C. §112(6), the parties dispute whether the corresponding structure is limited to archival storage devices including magnetic tape or CD ROM. Defendants contend that it is despite the fact that the specification expressly states that other storage device types

[114] Ex. 1 at p. 4.
[115] Ex. 8 at 29:51, 59; 30:57.
[116] Ex. 1 at p. 4
[117] Dkt. No. 228-2 at p. 77.
[118] Ex. 1 at p. 4.

may be used. [119] The specification recites other storage device types including RAM and hard drives. The specification also states that the invention may be written in these media in addition to CD ROM and magnetic tape.[120] Because RAM and hard drives are other disclosed storage devices, they are necessarily within the scope of a proper construction.

ix. "digital fingerprint"[121]

RPost agrees with Defendants that a message digest is one type of digital fingerprint disclosed in the specification. But the specification does not treat a message digest and a digital fingerprint as one and the same. It states "[t]he message digest is sometimes referred to as a "digital fingerprint" of the message x."[122] Indeed, the description of Figure 2A uses message digest and digital fingerprint in the alternative: "[i]n step 206, the system generates and stores a message digest or digital fingerprint generated from the message body."[123] Moreover, the specification acknowledges that "[o]ther known or new methods of detecting whether the contents of the message have been altered may be used."[124] Because RPost's construction encompasses the intended breadth of the invention, it should be adopted.

C. Terms of the '557 Patent

i. "A first verification" and "A second verification"[125]

The Court should adopt RPost's constructions of "a first verification" and "a second verification" because they are consistent with the intrinsic record. The specification describes hash values obtained by applying a hash function to some data

[119] Ex. 8 at 16:51-55.
[120] *Id.* at 27:36-38.
[121] Ex. 1 at p. 4.
[122] Ex. 8 at 7:66-67.
[123] *Id.* at 19:3-4.
[124] *Id.* at 7:52-54.
[125] Ex. 1 at p. 5.

input, such as an electronic message or an attachment to an electronic message.[126] The specification provides that verifiers "may constitute encrypted hashes of the message and of the attachment."[127] The plain language of unasserted claim 5 also indicates that the term "verification" encompasses an encrypted hash of the message and of the attachment.[128] The specification acknowledges that "[o]ther known or new methods of detecting whether the contents of the message have been altered may be used."[129] The absence of the encrypted hash limitation in asserted claim 1 demonstrates that "the first verification" and "the second verification" are not limited the encrypted hashes or other hashes of the message and the attachment.[130]

RPost agrees that a message digest (hash) or a digital fingerprint is one type of value that may be generated from data relating to the message or the attachment. But as noted above, the specification does not treat a message digest and a digital fingerprint as one and the same.[131] Further, the steps shown in Figure 9 distinguish between the hash/digital fingerprint and an encrypted hash, which, as noted above, may constitute a verification.[132] Thus, "a first verification" and "a second verification" cannot be limited to a hash or a digital fingerprint as Defendants propose.

ii. "The message is authenticated" and related terms[133]

For the same reasons discussed with the '372 patent, RPost's construction of the "authenticated" phrases of the '557 patent are consistent with the intrinsic record and should be adopted. The '557 patent repeatedly refers authentication in the context of

[126] Ex. 9 at 7:39-61.
[127] *Id.* at Abstract.
[128] *Id.* at 28:45-49.
[129] *Id.* at 7:37-39.
[130] *See Charles E. Hill & Assocs.*, 2012 U.S. Dist. LEXIS 3026, at *21-22.
[131] Ex. 9 at 7:51-52.
[132] *See, e.g.,* Ex. 9 at Fig. 9, steps 902-03.
[133] Ex. 1 at p. 5.

verifying the content and delivery of an electronic message.[134] Defendants' constructions are flawed because first, as noted above, the first verification and the second verification are not limited to a digital fingerprint or a hash. Second, Defendants improperly seek to read the comparing step from claim 5 into claim 1. The message and the attachment are authenticated in claim 1 by processing the message and the attachment and their respective verifications, which is broader than the comparing step recited in claim 5.[135] Finally, Defendants' construction requires comparing two digital fingerprints. But the embodiments disclosed in the specification, as claimed in claim 5, require comparing the message and the attachment and their respective verifications.[136]

VI. CONCLUSION

For the reasons above, RPost respectfully requests that the Court adopt RPost's constructions.

Respectfully submitted,

Dated: January 10, 2013

/s/ Robert P. Greenspoon
Robert P. Greenspoon
rpg@fg-law.com
Flachsbart & Greenspoon LLC
333 N. Michigan Ave., Suite 2700
Chicago, IL 60601-3901
Phone: (312) 551-9500
Fax: (312) 551-9501

Kenneth C. Goolsby
Boon, Shaver, Echols, Coleman
& Goolsby, PLLC
1800 NW Loop 281, Suite 303
Longview, Texas 75604
Phone – 903.759.2200
Fax – 903.759.3306

[134] Ex. 9 at 3:25-32.
[135] *Id.* at 28:62-65.
[136] *Id.*

Email: casey.goolsby@boonlaw.com

Attorneys for Plaintiff RMail Limited in 2:10-cv-258

Winston O. Huff
W. O. Huff & Associates PLLC
State Bar No. 24068745
302 N. Market St., Suite 450
Dallas, Texas 75202
214.749.1220 (office)
469.206.2173 (fax)
whuff@huffip.com

Lewis E. Hudnell, III
Colvin Hudnell LLP
375 Park Avenue Suite 2607
New York, New York 10152
Telephone: (347) 855-4772
Facsimile: (347) 772-3034
lewis@colvinhudnell.com

Attorneys for Plaintiffs RPost Holdings, Inc. RPost International Limited, and RMail Limited in 2:11-cv-16, 2:11-cv-64

Attorneys for Plaintiffs, RPost Holdings, Inc. RPost Communications Limited, and RMail Limited in 2:11-cv-299, 2:11-cv-300, 2:11-cv-325

CERTIFICATE OF SERVICE

I certify that on January 10, 2013 that I electronically filed the foregoing document with the Clerk of the Court and served all counsel and unrepresented parties of record deemed to have consented to electronic service using the CM/ECF system.

/s/ Robert P. Greenspoon